

(19)日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2000-276406

(P2000-276406A)

(43)公開日 平成12年10月6日 (2000.10.6)

(51)Int.Cl. ⁷	識別記号	F I	マーク* (参考)
G 06 F 12/14 3/06	3 2 0 3 0 1	G 06 F 12/14 3/06	3 2 0 A 5 B 0 1 7 3 0 1 A 5 B 0 6 5

審査請求 未請求 請求項の数5 OL (全14頁)

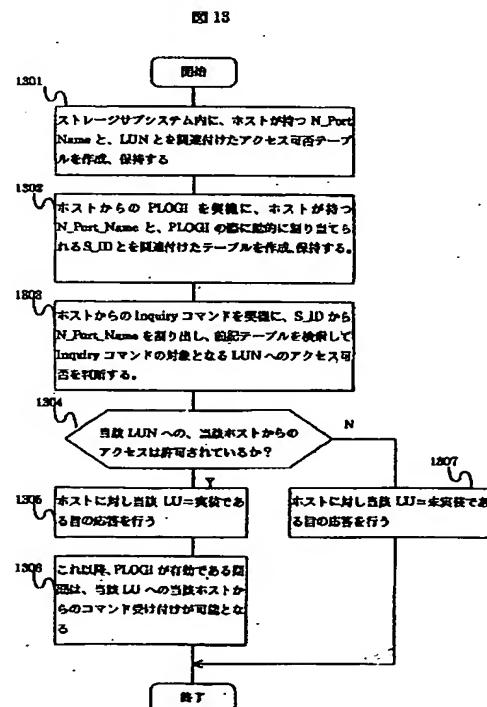
(21)出願番号	特願平11-85393	(71)出願人	000005108 株式会社日立製作所 東京都千代田区神田駿河台四丁目6番地
(22)出願日	平成11年3月29日 (1999.3.29)	(72)発明者	小笠原 裕 神奈川県小田原市国府津2880番地 株式会社日立製作所ストレージシステム事業部内
		(72)発明者	岡見 吉規 神奈川県小田原市国府津2880番地 株式会社日立製作所ストレージシステム事業部内
		(74)代理人	100068504 弁理士 小川 勝男 Fターム(参考) 5B017 AA01 BA01 BB03 BB06 CA09 CA16 5B065 CA01 CC01 PA02 PA04 PA13

(54)【発明の名称】 ファイバチャネル接続ストレージサブシステム及びそのアクセス方法

(57)【要約】

【課題】 ホストからストレージサブシステム内の記憶領域(LU)へのアクセスを選択的に制限することにより、不正アクセスを防止する。またこの際、アクセスの可否を判定する際生じるオーバヘッドが最小限となる方法を提供し、かつ判定の条件を標準ファイバチャネルプロトコルの範囲のみで行える方法を提供する。

【解決手段】 ホストのN_Port_NameあるいはNode_Nameとストレージサブシステム内のLUを関連付けるアクセス可否テーブル(1301)と、ホストがログインする際に割り当てるS_IDとLUとを関連付ける関連テーブル(1302)とを作成・保持し、ホストからのInquiry要求のS_IDと前記両テーブルとを用いてLUへのアクセス可否を判断し(1303)、ホストへ通知する(1304)。



【特許請求の範囲】

【請求項1】情報を記憶するドライブデバイスと、このドライブデバイスに情報を書き込み或いはこのドライブデバイスからの情報の読み込みを制御するデバイスドライブ制御部と、上位装置からのコマンドを受信するファイバチャネルインタフェースを持つポートと、前記コマンドに基づき前記デバイスドライブ制御部を制御して処理を行う演算装置とを備えたストレージサブシステムにおいて、

前記上位装置或いは上位装置のポートを識別する識別手段と前記ドライブデバイス内の特定の記憶領域とを関連付け前記上位装置から前記記憶領域に対するアクセス可否を定義したアクセス可否テーブルを設定するアクセス可否テーブル設定手段と、このアクセス可否テーブルを保持する保持手段とを備え、

前記演算装置は、前記上位装置からストレージサブシステムへの通信要求を受け付けた際にこの通信要求内の前記識別手段とフレームを送信するポートを識別するアドレス識別子とを関連付けた関連テーブルを設定し、この関連テーブルとドライブデバイスの実装状態を問い合わせるコマンドの前記アドレス識別子とから前記識別手段を割り出し、この識別手段と前記アクセス可否テーブルとから上位装置のアクセス可否を判断するストレージサブシステム。

【請求項2】前記演算装置は上位装置のアクセスを否と判断した場合には記憶領域が実装されていないという情報を上位装置に送信する請求項1に記載のストレージサブシステム。

【請求項3】情報を記憶するドライブデバイスと、このドライブデバイスに情報を書き込み或いはこのドライブデバイスからの情報の読み込みを制御するデバイスドライブ制御部と、上位装置からのコマンドを受信するファイバチャネルインタフェースを持つポートと、前記コマンドに基づき前記デバイスドライブ制御部を制御して処理を行う演算装置とを備えたストレージサブシステムにおいて、

前記上位装置からストレージサブシステムへの通信要求を受け付けた際にこの通信要求内の前記識別手段とフレームを送信するポートを識別するアドレス識別子とを関連付けた関連テーブルを設定する関連テーブル設定手段と、この関連テーブル及び前記上位装置或いは前記上位装置のポートを識別する識別手段と前記ドライブデバイス内の特定の記憶領域とを関連付け前記上位装置から前記記憶領域に対するアクセス可否を定義したアクセス可否テーブルとを保持する保持手段と、ドライブデバイスの実装状態を問い合わせるコマンドの前記アドレス識別子と前記関連テーブルとから割り出した前記識別子と前記アクセス可否テーブルとから上位装置のアクセス可否を判断する判断手段とを備えたストレージサブシステム。

【請求項4】前記アクセス可否テーブルは前記ポート毎に作成する請求項1乃至3の何れか1項に記載のストレージサブシステム。

【請求項5】前記上位装置或いは上位装置のポートを識別する識別手段とドライブデバイス内の特定の記憶領域とを関連付けこの記憶領域に対する上位装置のアクセス可否テーブルを作成・保持し、

前記上位装置からストレージサブシステムへの通信要求を受け付けた際に前記識別手段とフレームを送信するポートを識別するアドレス識別子とを関連付けた関連テーブルを作成・保持し、

この関連テーブルを用いてドライブデバイスの実装状態を問い合わせるコマンドの前記アドレス識別子から前記識別手段を割り出し、

割り出した識別手段と前記アクセス可否テーブルとを比較して前記上位装置のアクセス可否を判断するストレージサブシステムのアクセス方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、ANSI X3T11で標準化されたファイバチャネルプロトコルを、上位装置とのインタフェースとして持つストレージサブシステム（ディスクサブシステム）に係り、複数の上位装置からストレージサブシステム及びストレージサブシステム内の記憶領域へのアクセスを選択的に制限することにより、不正アクセスを防止できるストレージサブシステムに関する。

【0002】

【従来の技術】ANSI X3T11で標準化されたファイバチャネルプロトコルでは、多数の装置が接続可能であり、かつSCSI、ESCON、TCP/IP等多種のプロトコルを同時に運用可能な利点があるが、それに伴いセキュリティの確保が困難となる性質も併せ持っている。

【0003】ストレージサブシステムに対する不正アクセスを防止する方法としては、例えば特開平10-333839号公報では、ファイバチャネルプロトコルを用いた方法が開示されている。

【0004】この方法は、装置のインタフェース（ポートと呼ぶ）を、静的に一意に識別できるN_Port_Nameについて、上位装置を起動する前に予めストレージサブシステム中に記憶させ、かつこのN_Port_Nameと、ストレージサブシステム中の特定ポート、或いはN_Port_Nameとストレージサブシステム内部の任意の記憶領域とを関連付けるテーブルを保持し、上位装置起動後は、この上位装置がストレージサブシステムにアクセスする際に発行するフレームという情報単位の内部を、ストレージサブシステムにおいてフレーム毎に逐一判定して、フレーム内に格納されたN_Port_Nameがテーブル内に存在する場合にアクセスを許可し、存在しない場合はLS_RJTという接続拒否のフレームを上位に対して送出することによ

つて、前記テーブル内に存在しないN_Port_Nameをもつ上位装置からのアクセスを拒否するというものである。

【0005】

【発明が解決しようとする課題】しかし上記方法では、第一に接続可否の判定をフレーム毎に行う必要があるために通信性能が大幅に制限されること、第二にアクセス可否の対象がポートではなくストレージサブシステム内の部分領域である場合、上位装置から送出されるフレームすべてにN_Port_Nameを格納することが上位装置に要求されるため、上位装置側に標準ファイバチャネルプロトコル範囲外の仕様の実装を強いることから、実際の製品に適用することは困難である。

【0006】本発明はANSI X3T11で標準化されたファイバチャネルプロトコルを上位装置とのインターフェースとしてもつストレージサブシステムにおいて、上位装置からストレージサブシステム内の記憶領域へのアクセスを選択的に制限することにより、不正アクセスを防止することを目的とする。

【0007】またこの際、アクセスの可否を判定する際に生じるオーバヘッドが最小限となる方法を提供し、かつ判定の条件を標準ファイバチャネルプロトコルの範囲のみで行える方法を提供することを目的とする。

【0008】

【課題を解決するための手段】上記課題を解決するために、上位装置又は上位装置のポートを静的に一意に識別する識別手段であるN_Port_Name或いはNode_Nameと、ストレージサブシステム内におけるアクセス可否判定の対象である各記憶領域とを対応づけたテーブルをストレージサブシステム内に保持し、さらにN_Port_Name或いはNode_Nameと、上位装置がファイバチャネルインターフェースを用いてストレージサブシステムと通信を行う際に、上位装置又は上位装置のポートを一意に識別する手段として、情報の送受信に先立つログインプロセスにより動的に割り当てられる情報であるS_IDとを関連付けたテーブルをストレージサブシステム内に保持し、上位装置からストレージサブシステム内の記憶領域に対する情報取得要求が、Inquiryコマンドを用いて行われた契機で、要求フレームに含まれるS_IDを用いて、上記テーブルを検索及び比較することによって記憶領域に対するアクセス可否を判定する。

【0009】

【発明の実施の形態】以下、本発明の実施の形態について、図を用いて詳細に説明する。まず、本発明で使用するファイバチャネルの特徴について説明する。

【0010】ファイバチャネルは、独自のコマンドセットを持たないシリアルの転送方式をもつプロトコルであり、情報を同期に送るために伝送媒体の帯域幅を有効に利用できる特色を持っている。そして独自のコマンドセットを持たないかわりに、物理転送方式を、従来のSCSI、ESCONといったコマンドセットの運搬路として使用

することにより、従来のソフトウェア資産を継承しながら、より高速かつ多彩なデータ転送を可能としている。

【0011】ファイバチャネルはチャネルとネットワークの特長を併せ持つインターフェースである。すなわち、ファイバチャネルでは一旦転送元と転送先が確定すれば、遅延が少ない高速な転送が行える。これはチャネルの特長である。また、通信を希望する機器は、任意の契機でファイバチャネルの通信系に参加し、通信の目的となる相手の機器と相互に情報を交換することにより、互いを認識して通信を開始することができる。これはネットワークの特徴である。ここで述べた相手の機器との情報交換の手続きを、とくにログインと呼ぶ。

【0012】ファイバチャネルのインターフェースを持つ機器をノードと呼び、実際のインターフェースにあたる部分をポートと呼ぶ。ノードは1つ以上のポートを持つことが可能である。ファイバチャネルの系全体に同時に参加できるポートの数は、最大で24ビットのアドレスの数すなわち約1677万個である。この接続を媒介するハードウェアをファブリックと呼ぶ。送信元及び送信先のポートは、ファブリックを意識せずに互いのポートに関する情報のみを考慮して動作すればよいので、ファブリックを論理的な媒体として議論する場合も多い。

【0013】各ノード及びポートには、標準化団体から一定のルールによって割り当てられる世界中でユニークな識別子が記憶されている。これはTCP/IPのMACアドレスに相当するものであり、ハードウェア的に固定なアドレスである。このアドレスにはN_Port_Name、Node_Nameの2種類があり、それぞれ8バイトの領域を持つ。N_Port_Nameはポート毎に固有の値、Node_Nameはノード毎に固有の値となる。

【0014】ファイバチャネルでは、通信はOrdered Setと呼ばれる信号レベルの情報と、フレームと呼ばれる固定のフォーマットを持った情報とで行われる。

【0015】図1はこのフレームの構造を示している。フレーム101は、フレームの始まりを示すSOF (Start of Frame) 102と呼ばれる4バイトの識別子、リンク動作の制御やフレームの特徴づけを行う24バイトのフレームヘッダ103、実際に転送される目的となるデータ部分であるデータフィールド104、4バイトの巡回冗長コード(CRC) 105、フレームの終わりを示すEOF (End of Frame) 106と呼ばれる4バイトの識別子からなる。データフィールド104は0～2112バイトの間で可変である。

【0016】次に、図2を用いてフレームヘッダの内容について説明する。図2はフレームヘッダ202の詳細構造203における、1ワードの23-0ビット領域にあたるS_ID204のみ説明する。S_ID (Source ID) 204は当該フレームを送信するポートを識別するための3バイトのアドレス識別子であり、送受信されるすべてのフレームで有効な値を持つ。そして上位装置を動的に一意に識別できる情報

であり、PLOGI時（後述）に上位装置より報告される値である。このS_IDは動的に変動する値であり、FC_PHではファブリックによって初期化手続き時に割り当てられることになっている。割り当てられる値は、それぞれのポートが持つN_Port_Name、Node_Nameに依存する。

【0017】次に、送信元の機器と送信先の機器が互いに情報を交換する、ログイン手続きについて述べる。図3に、上位装置からストレージサブシステムへの通信要求であるPLOGIフレームの構造について示す。フレームヘッダ302の詳細構造304において、ワード1の23-0ビットがS_ID306である。また、データフィールド303の詳細構造305において、先頭から21バイト目～29バイト目までの8バイトの領域がN_Port_Name307を格納する領域であり、先頭から30バイト目～38バイト目までの8バイトの領域がNode_Name308を格納する領域である。

【0018】図4は、送信元（ログイン要求元）と送信先（ログイン要求先）との間に取り交わされる情報を示したものである。ファイバチャネルのログイン手続きには数種類があるが、ここではクラス3のログインで取り交わされる情報を示す。

【0019】ログイン要求元は、PLOGIフレーム403をログイン要求先へ送信する。このフレームには、ログイン要求元のN_Port_Name、Node_Name、S_ID及びその他の情報が含まれている。要求先の装置では、このフレームに含まれている情報を取り出し、ログインを受諾する場合はACC404と呼ばれるフレームをログイン要求元に対して送信する。

【0020】ログインを拒絶する場合は図5に示すように、PLOGIフレーム503に対して、ログイン受信先はLS_RJT504と呼ばれるフレームをログイン要求元に対して送信する。

【0021】ログイン要求元は、自らが送信したPLOGIフレームに対するACCフレームの応答を受信すると、ログインが成功したことを知り、データ転送などのI/Oプロセスを開始できる状態となる。LS_RJTを受信した場合はログインが成立しなかったため、ログイン要求先へのI/Oプロセスは不可となる。ここではクラス3のログインについて述べたが、他のログインにおいても、ログイン要求元からログイン要求先へ渡すことのできる情報の中に、N_Port_Name、Node_Name及びS_IDが含まれることは同様である。

【0022】次に、Inquiryコマンドについて説明する。Inquiryコマンドとは、I/Oプロセスを開始しようとする場合に先立ち、プロセスの対象となる論理デバイスに対して、その実装状態を問い合わせるコマンドである。例えば、上位装置からストレージサブシステムに含まれる記憶領域へのアクセス要求に先立つ情報問い合わせ要求のことである。本コマンドはSCSIでは必ずサポートされている標準コマンドである。

【0023】図6は、SCSI規格で定義されたInquiryコマ

ンドを、ファイバチャネル規格のフレームで送信する場合のフレーム601のフォーマットである。フレームヘッダ602の詳細構造604において、本フレームに先立つPLOGIで割り当てられたS_ID605が含まれている。データフィールド603にはFCP_LUN607、FCP_CNTL608、FCP_CDB609、FCP_DL610と呼ばれる領域がある。ここではFCP_LUN607、及びFCP_CDB609について述べる。

【0024】FCP_LUN607の中には、フレーム送信元が状態を問い合わせようとする、フレーム送信先のポートに関連付けられた論理ボリュームの識別子が格納されている。この識別子をLUNという。FCP_CDB609の中には、SCSIコマンドセットを使用する場合にはSCSIのコマンド記述ブロック（CDB）と呼ばれる命令情報が格納される。このFCP_CDB609の中に、SCSIのInquiryコマンド情報が格納されて、前述のFCP_LUN607と共に、フレーム要求先へ情報が転送される。

【0025】次に、Inquiryコマンドを受信したフレーム要求先が、問い合わせへの応答としてフレーム送信元へ返信する情報について述べる。この情報をInquiryデータと言う。図7にInquiryデータの抜粋を示す。ここでは、Inquiryデータ701のうちでクオифァイア702と、デバイス・タイプ・コード703の2つについて述べる。クオифァイア（Peripheral Qualifier）702は、指定された論理ユニットの現在の状態を設定する3ビットの情報である。

【0026】図8はビットパターンによって示される論理ユニットの状態を列挙したものである。コード000（2進）802は、論理ユニットとして接続されている装置がデバイス・タイプ・コード703の領域に示される種類の入出力機器であることを示している。本コードが設定されても、その論理ユニットが使用可能、すなわちレディ状態であることを必ずしも示しているわけではないが、その論理ユニットを使用できる可能性があるのは本コードが設定されている場合に限る。

【0027】コード001（2進）803は、論理ユニットとして接続されている装置がデバイス・タイプ・コード703の領域に示される種類の入出力機器であることを示しており、かつそのロジカルユニットには実際の入出力機器が接続されていないことを示している。これは例えばCD-ROMドライブが実装されているが、CD-ROMがドライブ内に挿入されていないような場合を示すことになる。コード011（2進）804は、指定された論理ユニットがサポートされていないことを示す。従って指定された論理ユニットに装置が割り当てられることはない。本コードが設定されるときは、デバイス・タイプ・コード領域703にはかならずIF（16進）が設定されることが条件になっている。

【0028】デバイス・タイプ・コード（Peripheral Device Type）703は、指定された論理ユニットに実際に割り当てられている入出力機器の種別を示す5ビットの

情報である。

【0029】図9に各デバイスタイプ902に対応するに16進のコード901を示す。図9に示されている情報のうち、未定義又は未接続のデバイス903を表す1F(16進)904が設定されると、Inquiryコマンド送信元が問い合わせたデバイスは未定義或いは未接続ということになり、当該論理ユニットは当該送信元からは使用できないことになる。

【0030】図10に、このInquiryコマンドを用いた論理ユニット問い合わせの手順を示す。論理ユニットにアクセスしようとする上位装置1001は、アクセスしようとする論理ユニットをもつストレージサブシステム1002に対し、Inquiryコマンドを含むフレーム1003を送信する。このフレームには、PLOGIで割り当てられた、上位装置のS_IDと、問い合わせを行う論理ユニットの識別子であるLUNが含まれている。なおここで、LUNについては、FCP_LUN領域の他に、FCP_CDB内のInquiryコマンド情報そのものの中にも設定することができる。どちらの値を使用しても得られる効果は同じであるが、本実施例ではLUNの値はFCP_LUNに格納された値を使用するものとする。

【0031】Inquiryコマンドを含むフレームを受信したストレージサブシステム1002は、問い合わせに対する返答に必要なInquiryデータを準備し、作成したInquiryデータを含むフレーム1004を上位装置に対して送信する。このときInquiryデータを格納するフレームを、FCP_DATAと呼ぶ。このとき、ストレージサブシステムが、問い合わせのあったロジカルユニット（論理ユニット）について、クオリファイア000（2進）、デバイスタイプ00~09（16進）のいずれかを設定した場合、このInquiryデータを受信した上位装置は、ロジカルユニットに対するI/Oを試みることが可能となる。

【0032】また、図11に示すように、ストレージサブシステム1102が、クオリファイア001（2進）又は011（2進）、デバイスタイプ1F（16進）を設定した場合、このInquiryデータ1104を受信した上位装置は、ロジカルユニットに対するI/Oが不可能であることを検出する。これらのことから、Inquiryデータに格納するクオリファイア、及びデバイス・タイプ・コードを管理することによって、上位装置からのロジカルユニットへのアクセスの許可及び不許可を制御することが可能となる。

【0033】本発明では、上位装置からのアクセスを許可、或いは拒否する対象として、ストレージサブシステム内の一定領域を選択することを可能としている。この領域は上位装置から明示的にアドレス指定が可能な領域であり、LU（Logical Unit）と呼ばれる。LUの識別子をLUN（Logical Unit Number）と呼ぶ。SCSI-2ではLUNの個数は1ターゲットあたり8である。

【0034】次に、本発明による処理の流れについて説明する。

【0035】図12は、本発明の実施例となる装置の構成図である。本装置をストレージサブシステム1201と呼ぶ。ストレージサブシステム1201は、複数のファイバチャネルインターフェースを持つポート1202によって上位装置（ホストと呼ぶ）1203と接続されている。接続形態はファイバチャネル規約によりさまざまであるが、本発明では接続形態を問わないため一括してファイバチャネル1204として表記してある。

【0036】上位装置1203もまたファイバチャネルインターフェースを持つポート1205を1つ以上備えており、それぞれのポート1205がストレージサブシステム1201上のポート1202とファイバチャネルプロトコルにより通信可能である。

【0037】ストレージサブシステム1201は中央演算装置1206を持ち、各種処理を行う。またストレージサブシステム1201は内部に不揮発メモリ1207を備えている。この不揮発メモリ1207は各種テーブルやN_Port_Name或いはNode_Nameを保持する保持手段としての役割を果たす。デバイスドライバ制御部1208はバス1209を介して情報を記憶しているドライブデバイスと接続されている。本図ではドライブデバイスを論理単位としてとらえ、論理ユニット（LU）1210として表示している。

【0038】また、ストレージサブシステム1201は通信制御部1211を持ち、通信回線1212を介して保守用装置1213の通信制御部1214と情報の送受信を行うことができる。保守用装置1213とは例えばパソコンのようなものであり、中央演算装置1215と入力手段1216及び表示手段1217を持つ。ユーザはこの保守用装置1213を用いて、ストレージサブシステム1201の保守を行う他、N_Port_Name或いはNode_NameとLU1210の特定の記憶領域とを関連付け上位装置1203に対するアクセス可否を定義した情報（アクセス可否テーブル）を設定する。このように保守用装置1213は設定手段の役割も果たす。不揮発メモリ1207はこのように定義したアクセス可否テーブルをN_Port_Name或いはNode_Nameと共に保持する。

【0039】更に不揮発メモリ1207は、中央演算装置1215で作成する関連テーブル（上位装置1203からストレージサブシステム1201への通信要求であるPLOGIを受け付けた際に、N_Port_Name或いはNode_Nameと上位装置1203とを動的に一意に識別できる情報であり、PLOGI時に上位装置1203より報告される値であるS_IDとを関連付け、このS_IDを不揮発メモリ1207内に保持してあるN_Port_Name或いはNode_Nameと関連付けたテーブル）を保持する。

【0040】図13は、本発明によるLUNセキュリティの実現方法の概要を説明したものである。まず手順1301では、ユーザは予めホストが持つN_Port_Nameを用いて、ストレージサブシステムの各ポート毎に関連付けられたLUNと、そこにアクセスしうるホストのN_Port_Nameを結び付けたアクセス可否テーブルを保守用装置（図12参

照)などを用いて作成し、ストレージサブシステム内の記憶領域(図12に示す不揮発メモリ等)に保持する。ここで得られるN_Port_Nameは既知であるとする。

【0041】次に、手順1302において、ホストがストレージサブシステムに対してログインを行う。ストレージサブシステムは、このログインのPLOGIフレームからホストのN_Port_Name及びS_IDを取り出し、N_Port_NameとS_IDとを関連付けた関連テーブルを作成する。作成された関連テーブルは、先のアクセス可否テーブルと同様にストレージサブシステム内の記憶領域に保持される。

【0042】次に、手順1303に移り、ホストはストレージサブシステム内の論理ユニットの状態を検査するためにInquiryコマンドを送信する。このInquiryコマンドを受信したストレージサブシステムは、Inquiryコマンドを格納しているフレームのヘッダからS_IDを取り出し、また同フレームからInquiryコマンドの対象となるLUNを取り出す。そして関連テーブルを使用して、S_IDからN_Port_Nameを割り出し、さらにアクセス可否テーブルからそのLUNがN_Port_Nameに対してアクセス許可されているか、もしくは不許可であるかの情報を取得する。

【0043】許可か不許可かの情報を用いて手順1304で中央演算装置はアクセス可否の判定をおこなう。結果が許可であった場合は、手順1305においてInquiryデータにLUが実装であることを設定し、不許可であった場合は、手順1307においてInquiryデータにLUが未実装であることを設定し、ホストに対して送信する。Inquiryデータを受信したホストはデータを解析し、対象LUが実装である、すなわち対象LUへのアクセスが許可されていることをデータから得ると、手順1306に示すように、それ以降当該LUに対してのI/O要求を行うことが出来るようになる。

【0044】対象LUが未実装であることを検出すると、それ以降当該LUへのI/O要求へのI/O要求を行うことはできない。以上の手順により、ストレージサブシステム内のLUに対するセキュリティの管理が実現できることになる。

【0045】尚、N_Port_Nameの代わりにNode_Nameを用いた場合も同様である。また、アクセス可否の判断は中央演算装置ではなく、専用の処理装置を設けて判断手段としてもよい。

【0046】次に、各手順について詳細に説明する。

【0047】まず、最初の手順であるN_Port_NameとLUNとの対応づけを行うテーブル作成手順について説明する。

【0048】本発明におけるLUNに対するセキュリティ情報は、ストレージサブシステムに存在するポートを単位として管理されるものとする。つまり、論理ユニットLUは各ポートに対して定義され、ホストはこれらのポートを通してLUへアクセスする。したがって、セキュリティ情報もポート単位で管理されることになる。この場合必要な情報は、ホストを一意に特定できる情報、各LUの

識別子であるLUN、及びLUNに対するアクセスの可否を示す状態ビットである。

【0049】ホストを一意に特定できる情報とは、この時点ではN_Port_Nameとなる。N_Port_Nameは、ホストに存在するポート毎にユニークな値であるので、本発明によればホストのポート毎に、ストレージサブシステムのポートにおけるLUに対するセキュリティを設定できることになる。N_Port_Nameの替わりに、Node_Nameを使用したテーブルを作成すれば、ホスト毎にセキュリティを設定することになる。LUに対するアクセス権限を与える対象がホストのポート毎であるか、ホスト毎であるかの相違があるので、本実施例ではN_Port_Nameについて説明する。すなわち本実施例ではホストのポート毎にセキュリティを設定する方法を述べるが、N_Port_Nameの記述をNode_Nameに読み替えることによって、容易にホスト単位のセキュリティ設定方式を得ることができる。また、本実施例では、ホスト上にあるポートのことを、簡略化のためにホストと呼ぶことにする。つまり、ホストという語はホストそのものと、ホスト上に存在するポートの双方、或いはいずれかを意味することになる。

【0050】図14に、本実施例で作成するアクセス可否テーブルを示す。本テーブルはストレージサブシステム上にあるポート毎に作成される。作成はストレージサブシステムと通信可能な保守用の装置から、入力手段とその入力結果を確認するための表示手段を用いて指示することにより行う。通信回線の種類により、LANを用いればストレージサブシステムに近い場所からの設定、電話回線を用いれば保守センタ等遠隔地からの設定が可能である。また内部バスを用いて保守用装置とストレージサブシステムを一体化させることも可能である。

【0051】LUN1402はポートに関連付けられたLUを示し、N_Port_Name1403の数はそのポート配下に存在するLUへアクセスする可能性のあるホストの数だけ存在する。LU及びホストの数は有限な数となる。テーブルの各要素において、本実施例では値"1"がアクセス許可を、値"0"がアクセス拒否を意味することにする。図14では当該ポートにおいて、LUN 0へアクセス許可があるホストは、N_Port_Name "0123456789ABCDEF" 1409 をもつホストのみであり、LUN 1 1405へアクセス許可があるホストは、N_Port_Name "01234567 89ABCDE" 1410及び"01234567 89ABCDEF" 1411をもつホストである。またLUN n-1 1407へのアクセスが許可されているホストは存在しない。

【0052】図15に示すように、本テーブルは、セキュリティの設定が必要なポートすべてについて作成し、ストレージサブシステム内の記憶領域に保持する。このとき記憶領域に不揮発記憶領域を使用すれば、ストレージサブシステムの電源が切断された場合でも情報を保持することができる。また、初期値を0又は1としてテーブルを作成しておくことにより、テーブル作成を簡略化する

ことができる。

【0053】次に、ホストからのログインの手順について詳細に説明する。本手順ではPLOGIに伴う情報から、ホストのN_Port_NameとホストのS_IDを結び付ける処理を行う。

【0054】まず、図16の手順1602に示すように、ホストからのログイン手続きとして、PLOGIフレームが送信される。手順1603においてストレージサブシステムでは、PLOGIフレームのヘッダから、ホストのS_IDを取得する。また同時に、手順1604において、PLOGIフレームのデータ領域から、ホストのN_Port_Nameを取得する。手順1605において、この2つの値を結び付け、図17に示すような関連テーブルを作成する。PLOGIはホストのポートと、ストレージサブシステム上のポートとの間で交わされるログインであるので、本テーブルもストレージサブシステムのポート毎に作成されることになる。

【0055】手順1606でテーブルを更新することによって、本テーブルを用いて、S_ID1701が与えられれば該当するN_Port_Name1702を得ることが可能となる。本テーブルも、ストレージサブシステム内の記憶領域に保持されることは図14で示したテーブルと同様である。ホストに対しては、手順1607でPLOGIに対する応答としてACCと呼ばれるフレームを送信し、ホストにログインが受理されたことを通知する。ACCフレームを受信したホストは、以降当該ポートに対してのInquiry等を発行することができるようになる。

【0056】次に、ホストからのInquiryコマンドの送信と、それに伴うセキュリティの応答について図18を用いて詳細に説明する。Inquiryコマンドは、FCP_CMNDと呼ばれる情報単位を含むフレームとしてホストからストレージサブシステムへ送信される。手順1802でホストからのデータフィールド内のFCP_CMNDフレームを受信したストレージサブシステムは、手順1803でFCP_CMNDフレームの内容を解析する。FCP_CMNDがInquiryコマンドでない場合は、それぞれに応じた処理1805に分岐する。FCP_CMNDがInquiryコマンドであった場合は、手順1806に遷移し、当該フレームからS_IDを切り出す。また、同時に手順1807にてFCP_LUNからInquiryが対象としているLUNを取り出す。

【0057】次に、手順1808に移り、フレームから切り出したS_IDから、図17で示したテーブルを用いてN_Port_Nameを求める。さらに、求めたN_Port_Nameについて、図14で示したテーブルより、Inquiryコマンドが対象としているLUNについて、セキュリティを示したビットの状態を取得する。この時ホストから得られたS_IDが、FF FF01であり、Inquiryの要求するLUNが0であったとする。まず手順1808にて、図17に示すテーブルよりS_IDFF FF01 1703に対応するN_Port_Name "01234567 89ABCDEF" 1706を取得した後、手順1809に移り図14に示したテーブルよりN_Port_Name "01234567 89ABCDEF" 1409に対する

るLUN 0 1404のセキュリティ "1" を得る。

【0058】セキュリティ "1" は本実施例ではアクセス許可を意味するので、手順1811に分岐し、ホストへ報告するInquiryデータとして、クオリファイアに000 (2進)、デバイスタイプに当該デバイスに対応するコードをセットする。例えばストレージサブシステムがハードディスクアレイサブシステムである場合は、デバイスタイプは00 (16進) となる。ついでInquiryデータを格納したフレームを作成し、手順1813でホストに対して送信をおこなう。さらに手順1814にて、返信が終了したことを示すFCP_RSPと呼ばれるフレームをホストに対して送信する。

【0059】この一連の返信データを受け取ったホストは、Inquiryの結果として当該LUN=0のLUに対してアクセスができるることを検知したことになるため、以降は次回のInquiryコマンドを受け付けるまで、当該LUに対してセキュリティのチェックを行う必要なくアクセスを行うことが可能となる。

【0060】次にアクセスを拒否する場合を説明する。Inquiryコマンドの送信によりホストから得られたS_IDがFFFF01であり、Inquiryの要求するLUNが1であったとする。手順1808において、図17に示す関連テーブルよりS_IDFFFF011703に対応するN_Port_Name "01234567 89ABCDEF" 1706を取得した後、図14に示すアクセス可否テーブルよりN_Port_Name "01234567 89ABCDEF" 1409に対するLUN 1 1405のセキュリティ "0" を得る。

【0061】セキュリティ "0" は本実施例ではアクセス拒否を意味するので、手順1812へ分岐し、ホストへ報告するInquiryデータとして、クオリファイアに001 (2進) 又は011 (2進)、デバイス・タイプ・コードに1F (16進) をセットしたInquiryデータを作成する。このInquiryデータを受信し、ついでFCP_RSPを受信したホストは、Inquiryの結果として当該LUN=1のLUが未実装であるという情報を得る。したがって、以降ホストは当該LUが実装されていないと判断するのでアクセス要求をすることはなくなる。

【0062】以上のようにして、N_Port_Name、S_ID、LUNを用いたテーブルを保持することで、ストレージサブシステム側のポート毎に、ホストの各ポートに対しての各LUNへのアクセスについてのセキュリティを、ログイン及びInquiryの際に判断することで、効率よく行うことができる。

【0063】

【発明の効果】本発明によって、上位装置から特定LUNに対するアクセスを、予め設定してあるN_Port_NameあるいはNode_NameとLUNとのアクセス可否テーブル、PLOGIの際に判明するN_Port_NameあるいはNode_NameとS_IDとの関係を用いて作成した関連テーブルの双方のテーブルを用いることによって、上位装置あるいは上位装置のポートからのLUへの状態問い合わせがあった時点でアクセス可

否を決定し返答することができるため、ストレージサブシステムへのアクセス制限を、LUN単位で、しかも初回のみの判定プロセスで行うことができ、ファイバチャネル及びSCSIの規格上最も分解能の高いセキュリティを、高いパフォーマンスで確保することができる。

【図面の簡単な説明】

【図1】ファイバチャネルプロトコルにおけるフレームの構造図である。

【図2】フレームヘッダの構造図である。

【図3】PLOGIフレームの構造図である。

【図4】PLOGIが受諾されるシーケンス図である。

【図5】PLOGIが拒否されるシーケンス図である。

【図6】SCSIのInquiryコマンドを含むフレームの構造図である。

【図7】Inquiryデータの構造図である。

【図8】Inquiryデータ中クオリファイアの内容定義図である。

【図9】Inquiryデータ中デバイス・タイプ・コードの内容定義図である。

【図10】InquiryデータにLU通常状態が設定される場合のシーケンス図である。

【図11】InquiryデータにLU未定義状態が設定される場合のシーケンス図である。

【図12】ストレージサブシステムの構成図である。

【図13】全体シーケンスのフローチャートである。

【図14】N_Port_Nameに対するLUアクセス可否の定義テーブルである。

【図15】LUアクセス可否定義テーブルの設定フローチャートである。

【図16】PLOGI処理のフローチャートである。

【図17】ホストN_Port_NameとS_IDを関連付けるテーブルである。

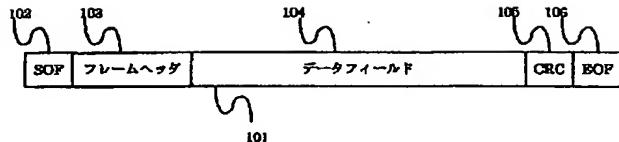
【図18】Inquiryコマンド処理のフローチャートである。

【符号の説明】

101…フレーム、102…SOF (Start of Frame)、103…フレームヘッダ、104…データフィールド、105…CRC、106…EOF (End of Frame)、201…フレーム、202…フレームヘッダ、203…フレームヘッダ詳細、204…S_ID、301…フレーム、302…フレームヘッダ、303…データフィールド、304…フレームヘッダ詳細、305…データフィールド詳細、306…S_ID、307…N_Port_Name、308…Node_Name、401…ログイン要求元の動作、402…ログイン受信先の動作、403…PLOGIフレームの内容、404…ACCフレーム、501…ログイン要求元の動作、502…ログイン受信先の動作、503…PLOGIフレームの内容、504…LS_RJTフレーム、601…フレーム、602…フレームヘッダ、603…データフィールド、604…フレームヘッダ詳細、605…S_ID、606…データフィールド詳細 (FCP_CMND)、607…FCP_LUN、608…FCP_CNTL、609…FCP_CDB (Inquiry)、610…FCP_DL、701…Inquiryデータ抜粋、702…クオリファイア、703…デバイス・タイプ・コード、801…クオリファイアの定義、802…000 (2進)、803…001 (2進)、804…011 (2進)、901…デバイス・タイプ・コード (16進)、902…デバイス・タイプ、903…1F (16進)、904未定義又は未接続のデバイス、1001…上位装置 (ホスト) のInquiry処理シーケンス、1002…ストレージサブシステムのInquiry処理シーケンス、1003…Inquiryを含むフレーム (FCP_CMND) に格納される情報、1004…デバイス通常状態を通知するInquiryデータ、1101…上位装置 (ホスト) のInquiry処理シーケンス、1102…ストレージサブシステムのInquiry処理シーケンス、1103…Inquiryを含むフレーム (FCP_CMND) に格納される情報、1104…デバイス未定義状態を通知するInquiryデータ、1201…ストレージサブシステム、1202…ストレージサブシステムのファイバチャネルポート、1203…上位装置 (ホスト)、1204…ホストとストレージサブシステムを接続するファイバチャネルプロトコル、1205…ホストのファイバチャネルポート、1206…中央演算装置、1207…不揮発メモリ、1208…デバイスドライブ制御部、1209…バス、1210…LU (論理ユニット)、1211…通信制御部、1212…通信回線、1213…保守用装置、1214…通信制御部、1215…中央演算装置、1216…入力手段、1217…表示手段、1301…全体手順1、1302…全体手順2、1303…全体手順3、1304…全体手順4、1305…全体手順5、1306…全体手順6、1307…全体手順7、1401…N_Port_Nameに対するLUアクセス可否定義テーブル、1402…LUN、1403…N_Port_Name、1404…LUN 0のLUに対する定義、1405…LUN1のLUに対する定義、1406…LUN 2のLUに対する定義、1407…LUN n-1のLUに対する定義、1408…LUN nのLUに対する定義、1409、1410、1411…N_Port_Name、1601…PLOGI処理フローチャート開始、1602…PLOGI処理手順1、1603…PLOGI処理手順2、1604…PLOGI処理手順3、1605…PLOGI処理手順4、1606…PLOGI処理手順5、1607…PLOGI処理手順6、1701…S_ID、1702…N_Port_Name、1703、1704、1705…S_ID、1706、1707、1708…N_Port_Name、1801…Inquiry処理フローチャート開始、1802…Inquiry処理手順1、1803…Inquiry処理手順2、1804…Inquiry処理手順3、1805…Inquiry処理手順4、1806…Inquiry処理手順5、1807…Inquiry処理手順6、1808…Inquiry処理手順7、1809…Inquiry処理手順8、1810…Inquiry処理手順9、1811…Inquiry処理手順10、1812…Inquiry処理手順11、1813…Inquiry処理手順12、1814…Inquiry処理手順13。

【図1】

図1



101

102

103

104

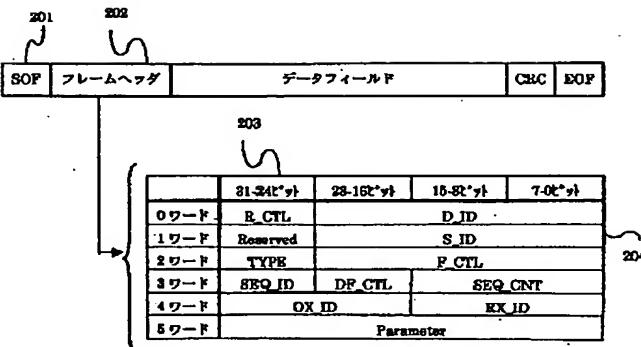
105

106

図1

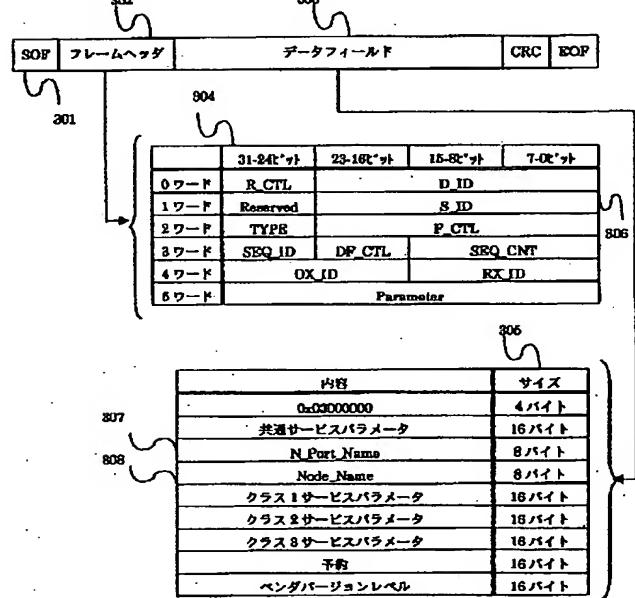
【図2】

図2



【図3】

図3



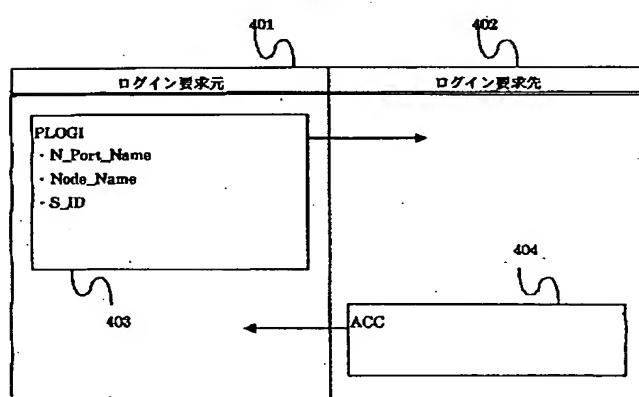
【図7】

図7

位置	内容
0バイト	3197747 (32ビット) アダルト・キッズ・キッズ (64ビット) (以下略)
1バイト	—
...	—

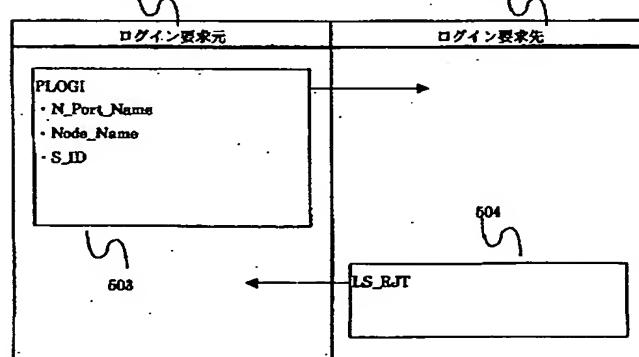
【図4】

図4



【図5】

図5

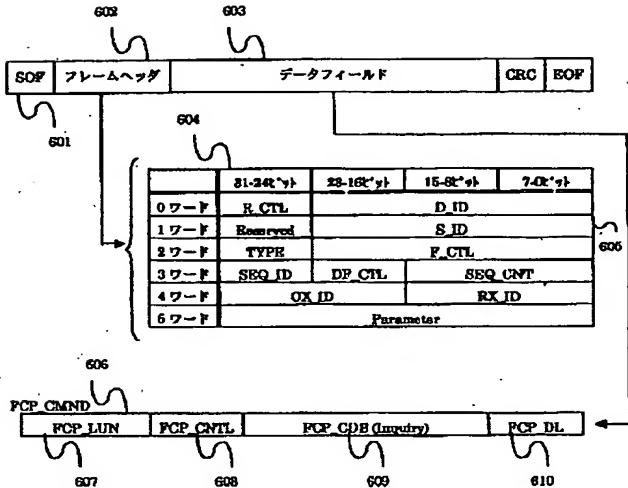


【図7】

図7

【図6】

図6



【図9】

図9

コード (16進)		デバイス・タイプ
00h		ダイレクト・アクセス・デバイス (例: 磁気ディスク)
01h		シーケンシャル・アクセス・デバイス (例: 磁気テープ)
02h		プリンタ・デバイス
03h		プロセッサ・デバイス
04h		ライト・ワンス・デバイス (例: 透過程型光ディスク)
05h		CD-ROM デバイス
06h		スキャナ・デバイス
07h		光メモリ・デバイス (例: イレーザブル光ディスク)
08h		メディア・エンジニア・デバイス (例: 磁気テープ (または光ディスク) ライブライ)
09h		コミュニケーション・デバイス (例: 通信回線)
0Ah~0Bh		(グラフィック装置用に定義予定)
0Ch~1Eh		(リザーブ)
1Fh		未定義または未接続のデバイス

【図8】

図8

コード (2進)	ロジカル・ユニットの状態
000	ロジカル・ユニットとして定義されている駆動は、デバイス・タイプ・コード・フィールドに示される種類の入出力機器である (ただし、そのロジカルユニットがレディ状態であることを示すものではない)。
001	ロジカル・ユニットは、デバイス・タイプ・コード・フィールドに示される種類の入出力機器であるが、そのロジカル・ユニットには、実際の入出力機器は接続されていない。
011	指定されたロジカル・ユニットはサポートされていない。

804

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

801

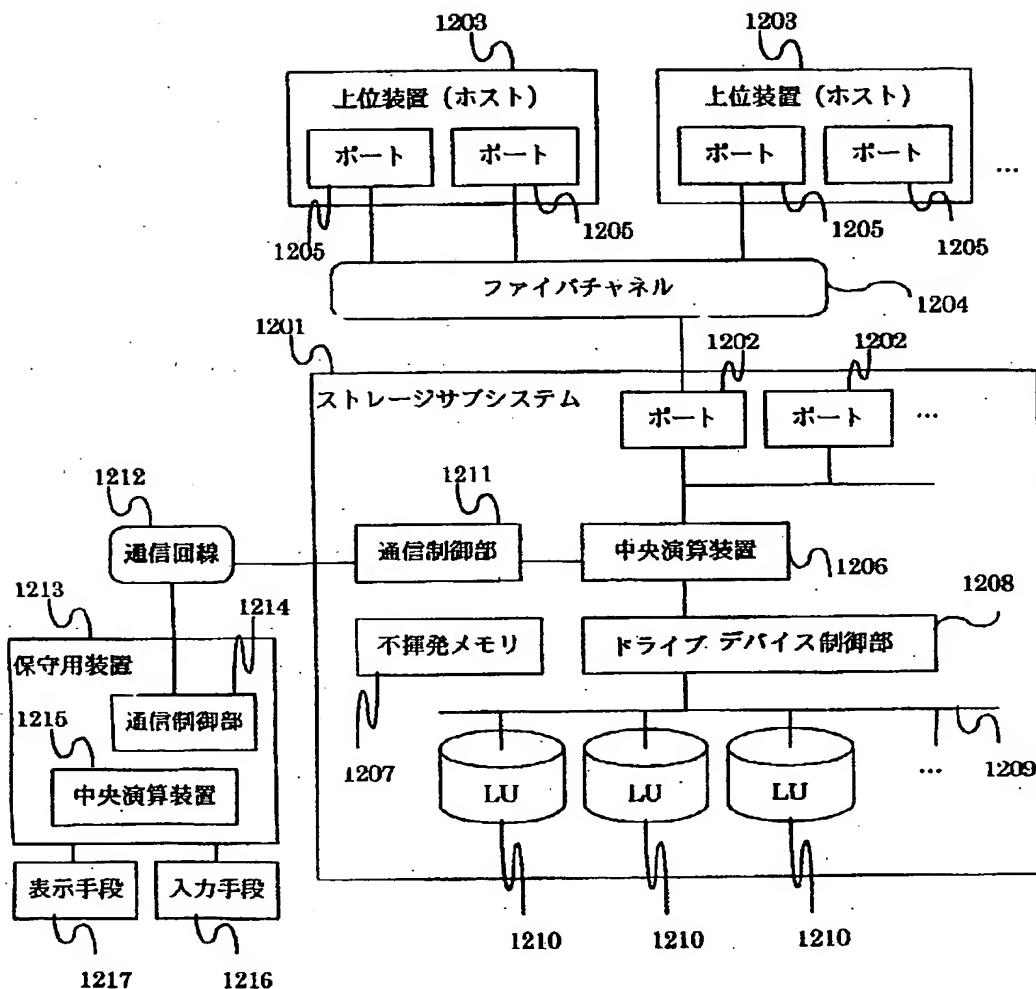
801

801

801

【図12】

図12



【図14】

図14

LUN					N_Port_Name
0	1	2	--	--	0123456789ABCDEP
1	0	0	--	0	0123456789ABCDEE
0	1	0	--	0	0123456789ABCDEB
0	1	1	--	0	0123456789ABCDED
--	--	--	--	--	--

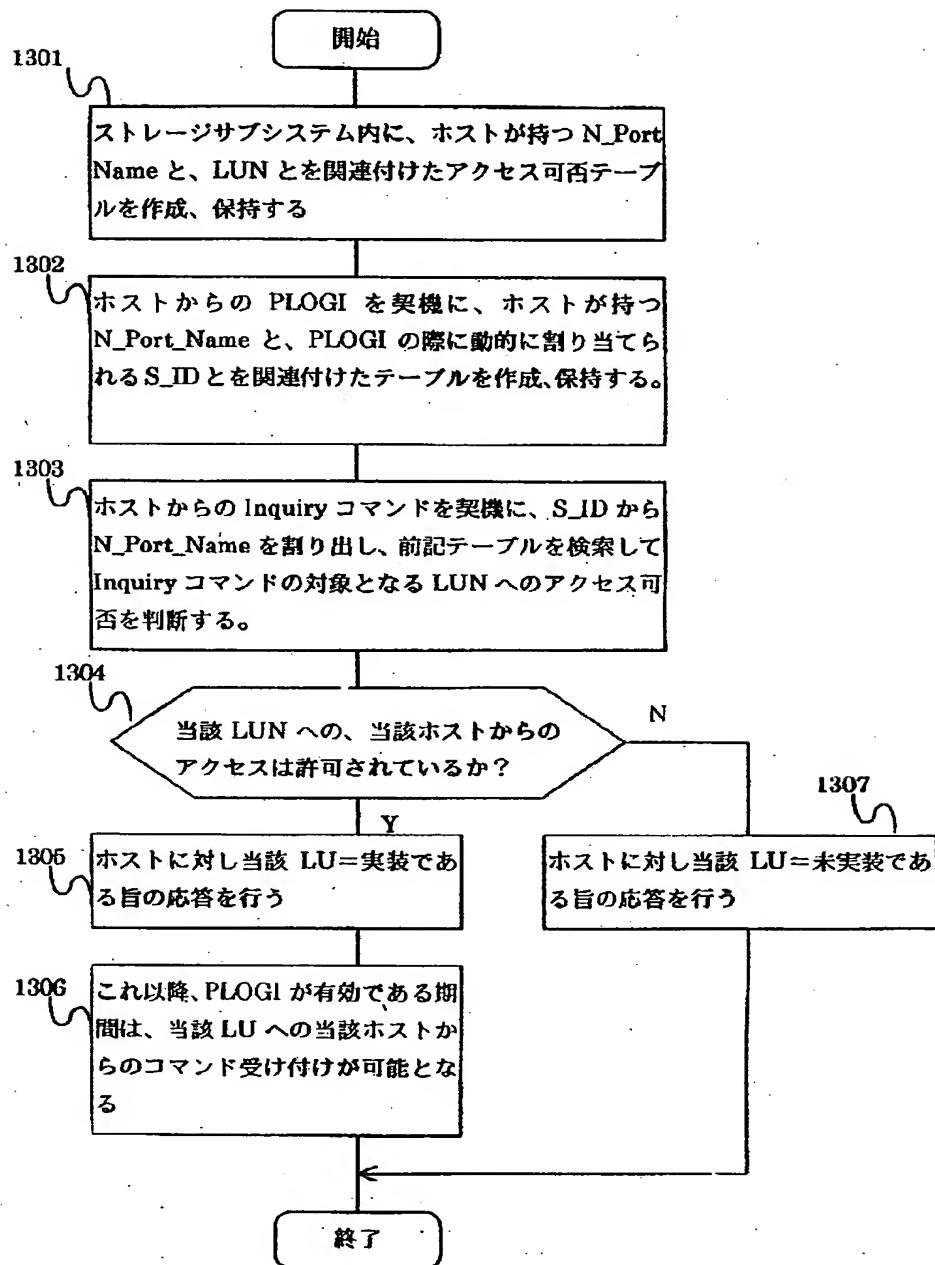
【図17】

図17

S_ID	N_Port_Name
FFFF01	0123456789ABCDEF
FFFF02	0123456789ABCDEE
FFFF03	0123456789ABCDED
--	--

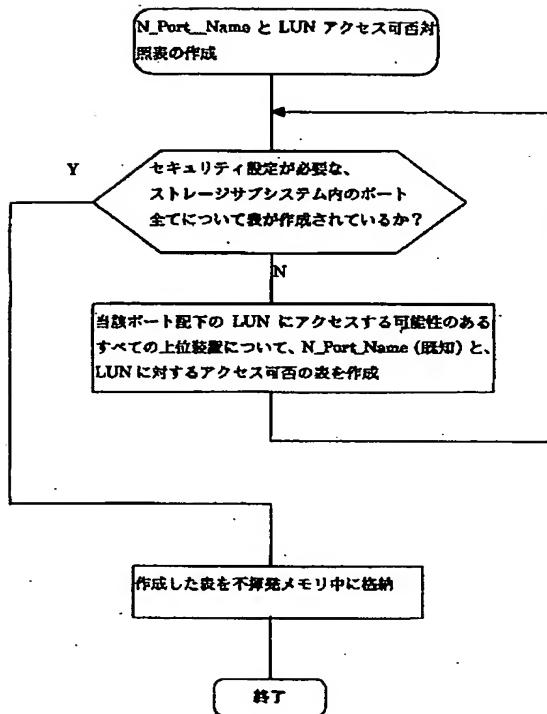
【図13】

図13



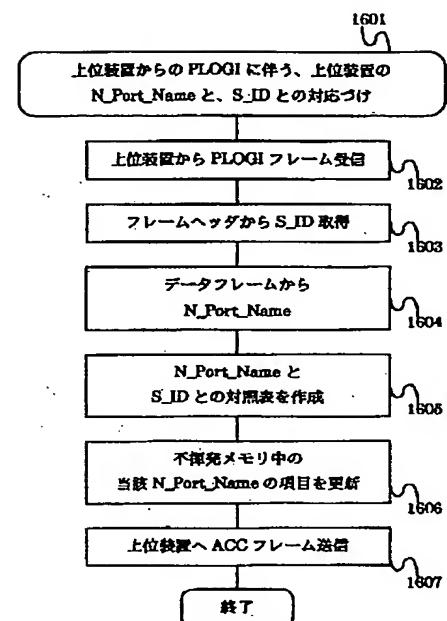
【図15】

図15



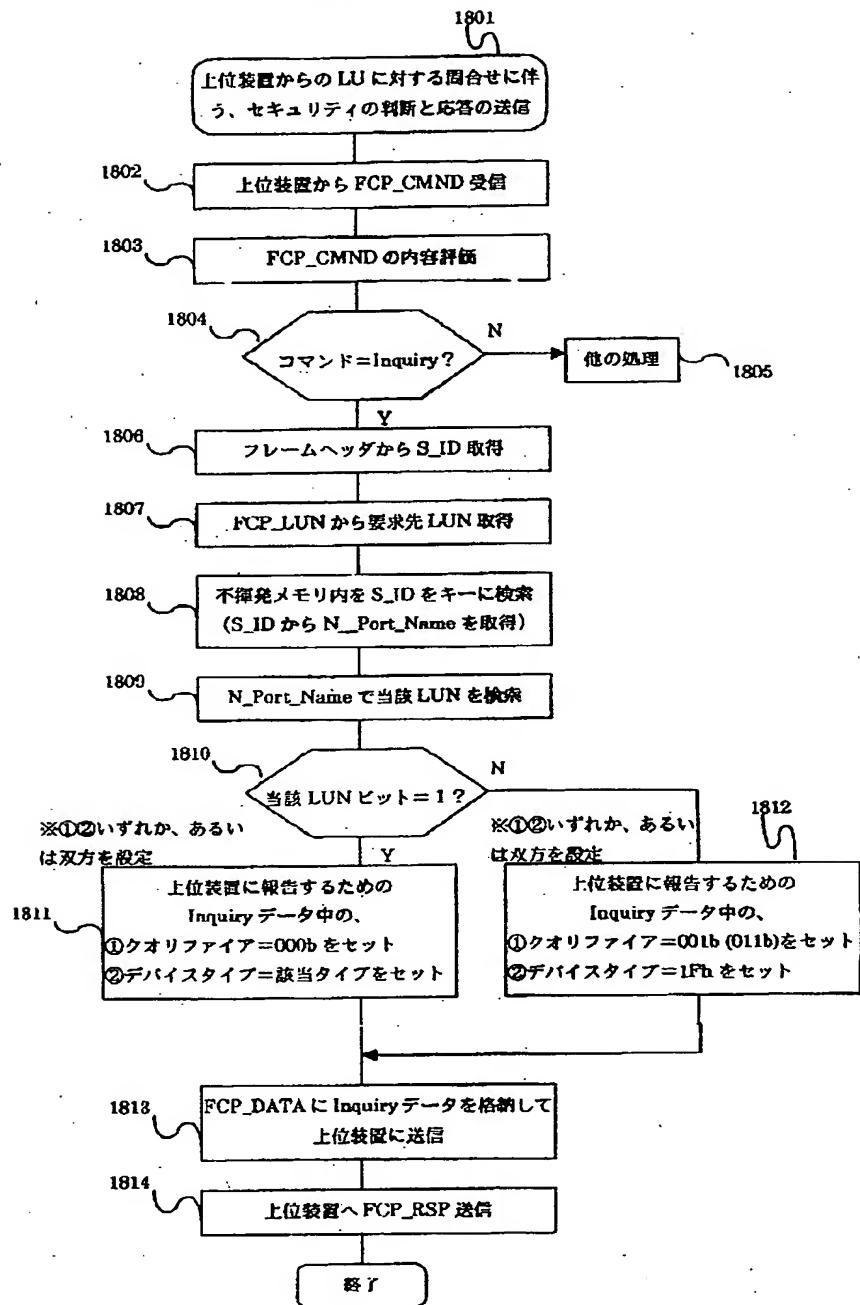
【図16】

図16



【図18】

図18



PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-276406
 (43)Date of publication of application : 06.10.2000

(51)Int.CI. G06F 12/14
 G06F 3/06

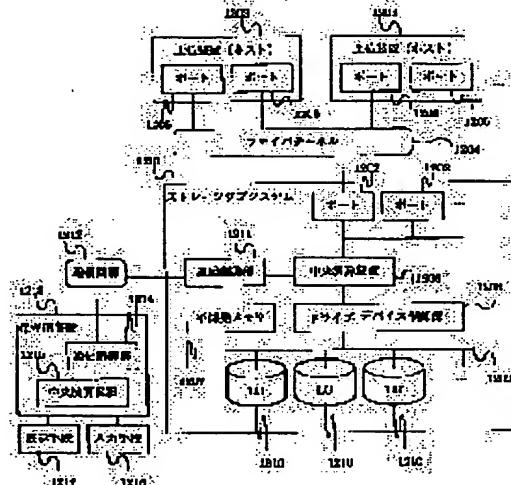
(21)Application number : 11-085393 (71)Applicant : HITACHI LTD
 (22)Date of filing : 29.03.1999 (72)Inventor : OGASAWARA YUTAKA
 OKAMI YOSHINORI

(54) FIBER CHANNEL CONNECTION STRAGE SUBSYSTEM AND ITS ACCESS MEMORY

(57)Abstract:

PROBLEM TO BE SOLVED: To prevent illegal access by selectively limiting access from a host device to a storage area in a storage subsystem.

SOLUTION: The storage subsystem 1201 is connected to the host device 1203 by a port 1202 which has multiple fiber channel interfaces. The storage subsystem 1201 has a communication control part 1211 and sends and receives information to and from a communication control part 1214 of a device 1213 for maintenance through a communication line 1212 to maintain the storage subsystem 1201 and also set whether or not the host device 1203 is allowed to gain access by relating N-Port-Name and a specific storage area of LU 1210 with each other. Through the setting, access from the host device 1203 to the specific storage area in the storage subsystem 1201 is selectively limited. Consequently, illegal access can be prevented.



LEGAL STATUS

[Date of request for examination] 13.05.2002
 [Date of sending the examiner's decision of rejection]
 [Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
 [Date of final disposal for application]
 [Patent number]
 [Date of registration]
 [Number of appeal against examiner's decision of rejection]
 [Date of requesting appeal against examiner's decision of rejection]
 [Date of extinction of right]

* NOTICES *

Japan Patent Office is not responsible for any damages caused by the use of this translation.

1. This document has been translated by computer. So the translation may not reflect the original precisely.
2. **** shows the word which can not be translated.
3. In the drawings, any words are not translated.

CLAIMS

[Claim(s)]

[Claim 1] The device drive control section which writes information in the drive device which memorizes information, and this drive device, or controls reading of the information from this drive device, In the storage subsystem equipped with the port with the fiber channel interface which receives the command from high order equipment, and the arithmetic unit which processes by controlling said device drive control section based on said command An access propriety table set up means to set up the access propriety table which associated a discernment means to identify the port of said high order equipment or high order equipment, and the specific storage region in said drive device, and defined the access propriety to said storage region from said high order equipment, It has a maintenance means to hold this access propriety table. Said arithmetic unit The association table which associated the address identifier which identifies the port which transmits said discernment means and frame in this communication link demand when the communication link demand to a storage subsystem from said high order equipment is received is set up. The storage subsystem which deduces said discernment means from said address identifier of the command which asks the mounting condition of this association table and a drive device, and judges the access propriety of high order equipment from this discernment means and said access propriety table.

[Claim 2] Said arithmetic unit is a storage subsystem according to claim 1 which transmits the information that the storage region is not mounted when access of high order equipment is judged to be no to high order equipment.

[Claim 3] The device drive control section which writes information in the drive device which memorizes information, and this drive device, or controls reading of the information from this drive device, In the storage subsystem equipped with the port with the fiber channel interface which receives the command from high order equipment, and the arithmetic unit which processes by controlling said device drive control section based on said command An association table setting means to set up the association table which associated the address identifier which identifies the port which transmits said discernment means and frame in this communication link demand when the communication link demand to a storage subsystem from said high order equipment is received, A maintenance means to hold the access propriety table which associated a discernment means to identify the port of this association table and said high order equipment, or said high order equipment, and the specific storage region in said drive device, and defined the access propriety to said storage region from said high order equipment, The storage subsystem equipped with a decision means to judge the access propriety of high order equipment from said identifier deduced from said address identifier and said association table of the command which asks the mounting condition of a drive device, and said access propriety table.

[Claim 4] Said access propriety table is a storage subsystem given in claim 1 created for said every port thru/or any 1 term of 3.

[Claim 5] Associate a discernment means to identify the port of said high order equipment or high order equipment, and the specific storage region in a drive device, and the access propriety table of the high order equipment to this storage region is created and held. The association

table which associates the address identifier which identifies the port which transmits said discernment means and frame when the communication link demand to a storage subsystem from said high order equipment is received is created and held. Said discernment means is deduced from said address identifier of the command which asks the mounting condition of a drive device using this association table. The access approach of a storage subsystem of comparing the deduced discernment means with said access propriety table, and judging the access propriety of said high order equipment.

[Translation done.]

* NOTICES *

Japan Patent Office is not responsible for any damages caused by the use of this translation.

1. This document has been translated by computer. So the translation may not reflect the original precisely.

2. **** shows the word which can not be translated.

3. In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention] This invention relates to the storage subsystem (disk subsystem) which has the fiber channel protocol standardized by ANSI X3T11 as an interface with high order equipment, and relates to the storage subsystem which can prevent unlawful access by restricting alternatively access to the storage region in a storage subsystem and a storage subsystem from two or more high order equipments.

[0002]

[Description of the Prior Art] In the fiber channel protocol standardized by ANSI X3T11, although much equipments can be connected and there is an advantage which can be applied to coincidence about the protocol of varieties, such as SCSI, ESCON, and TCP/IP, it also has the property in which reservation of security becomes difficult in connection with it.

[0003] As an approach of preventing unlawful access to a storage subsystem, the approach which used the fiber channel protocol is indicated, for example by JP.10-33839.A.

[0004] Before this approach starts high order equipment, it is made to memorize in a storage subsystem beforehand about N_Port_Name which can identify the interface (it is called a port) of particular port in a storage subsystem, or N_Port_Name and the storage region of the arbitration inside a storage subsystem. After high order equipment starting The interior of an information unit called the frame published in case equipment besides accesses a storage subsystem is judged in detail for every frame in a storage subsystem. By permitting access, when N_Port_Name stored in the frame exists in a table, and sending out the frame of a connection refusal called LS_RJT to a high order, when it does not exist Access from high order equipment with N_Port_Name which does not exist in said table is refused. It is.

[0005] [Problem(s) to be Solved by the Invention] However, the thing for which the communication link engine performance is sharply restricted by the above-mentioned approach since it is necessary to judge connection propriety for every frame in the first place. Since high order equipment is required to store N_Port_Name in all the frames sent out to the second from high order subsystem, it is difficult to apply to an actual product from forcing a high order equipment side mounting of the specification outside the standard fiber channel protocol range.

[0006] This invention aims at preventing unlawful access in the storage subsystem which has the fiber channel protocol standardized by ANSI X3T11 as an interface with high order equipment by restricting alternatively access to the storage region in a storage subsystem from high order equipment.

[0007] Moreover, it aims at offering the approach that how the overhead produced in case the propriety of access is judged serves as the minimum is offered, and the conditions of a judgment can be performed only in the range of a standard fiber channel protocol in this case.

[0008] [Means for Solving the Problem] N_Port_Name or Node_Name which is a discernment means to

identify statically the port of high order equipment or high order equipment uniquely in order to solve the above-mentioned technical problem. The table which matched each storage region which is the object of the access propriety judging in a storage subsystem is held in a storage subsystem. Further N_Port_Name or Node_Name. In case high order equipment communicates with a storage subsystem using a fiber channel interface, as a means to identify the port or high order equipment or high order equipment uniquely The table which associated S_ID which is the information dynamically assigned by the login process before information transmission and reception is held in a storage subsystem. S_ID contained in a demand frame is used from high order equipment by the opportunity to which the information acquisition demand to the storage region in a storage subsystem was given using the Inquiry command, and the access propriety to a storage region is judged by searching and comparing the above-mentioned table.

[0009]

[Embodiment of the Invention] Hereafter, the gestalt of operation of this invention is explained to a detail using drawing. First, the description of the fiber channel used by this invention is explained.

[0010] A fiber channel is a protocol with the serial transmittal mode without an original commands set, and in order to send information to asynchronous, it has the special feature which can use the bandwidth of a transmission medium effectively. And a high speed and variegated data transfer are made possible more, inheriting the conventional software property by using the physical transmittal mode for instead of [without an original commands set] as a haulageway of commands sets, such as the conventional SCSI and ESCON.

[0011] A fiber channel is an interface which has a channel and the network features. That is, by the fiber channel, once the source and the destination are decided, the high-speed transfer with little delay can be performed. This is the features of a channel. Moreover, by participating in the communication system of a fiber channel by the opportunity of arbitration, and exchanging information for the device of the partner who becomes the communicative purpose, and mutual, the device which wishes to communicate can recognize each other and can start a communication link. This is the network description. The procedure of information interchange with the device of the partner who stated here is called especially a log in.

[0012] The part which hits a node, a call, and an actual interface in a device with the interface of a fiber channel is called a port. A node can have one or more ports. The number of the ports which can participate in the whole system of a fiber channel at coincidence is the number of the 24-bit addresses, i.e., about 16,770,000 pieces, at the maximum. The hardware which carries this connection is called a fabric. Since a transmitting agency and the port of a transmission place should just operate only in consideration of the information about a mutual port, without being conscious of a fabric, they argue about a fabric as a logical medium in many cases.

[0013] The unique identifier is memorized all over the world assigned by the fixed Ruhr from a standardization organization in each node and a port. This is equivalent to the MAC Address of TCP/IP, and is the address [**** / in hardware]. There are two kinds of these addresses, N_Port_Name and Node_Name, and it has the field which is 8 bytes, respectively in them. For every port, N_Port_Name serves as a value of a proper for every node, and Node_Name serves as a value of a proper.

[0014] A communication link is performed by the fiber channel for the information on the signal level called Ordered Set, and information with a format of the immobilization called a frame.

[0015] Drawing 1 shows the structure of this frame. A frame 101 consists of 4 bytes of identifier called 4 bytes of identifier called SOF (Start of Frame) 102 which shows the beginning of a frame, 24 bytes of frame header 103 which performs control of link motion, and characterization of a frame, the cyclic redundancy code (CRC) 105 of 104 or 4 bytes of data field which is a part for the data division used as the purpose actually transmitted and EOF (End of Frame) 106 which shows the end of a frame. A data field 104 is adjustable among 0-2112 bytes.

[0016] Next, the contents of the frame header are explained using drawing 2. Drawing 2 shows the structure of a frame header. Here, only S_ID 204 which hits 1-word 23 -0-bit field in the detail structure 203 of the frame header 202 is explained. S_ID (Source ID) 204 is 3 bytes of address identifier for identifying the port which transmits the frame concerned, and has an

effective value with all the frames transmitted and received. And it is the information which can identify high order equipment uniquely dynamically, and is the value reported from high order equipment at the time of PLOGI (after-mentioned). This *S_ID* is a value changed dynamically and the fabric is to assign it by FC_PPH at the time of initialization procedure. It depends for the value assigned on *N_Port_Name* and *Node_Name* which each port has.

[0017] Next, the device of a transmitting agency and the device of a transmission place describe the log in procedure which exchanges information mutually. This structure of the PLOGI frame which is the communication link demands to a storage subsystem from high order equipment is shown in drawing 3. In the detail structure 304 of the frame header 302, 23 - 0 bit of WORD 1 is *S_ID*308. Moreover, in the detail structure 305 of a data field 303, 8 bytes of field from a head to 21st byte - the 29th byte is a field which stores *N_Port_Name*307, and 8 bytes of field from a head to 30th byte - the 38th byte is a field which stores *Node_Name*308.

[0018] Drawing 4 shows the information exchanged between transmission places (log in demand place) a transmitting agency (log in demand origin). Although there are some kinds in the log in procedure of a fiber channel, the information exchanged by the log in of a class 3 here is shown. [0019] Log in demand origin transmits the PLOGI frame 403 to a log in demand place. The information on *N_Port_Name* of log in demand origin, *Node_Name*, *S_ID*, and others is included in this frame. With the equipment of a demand place, the information included in this frame is taken out, and when accepting a log in, the frame called ACC404 is transmitted to log in demand origin.

[0020] When refusing a log in, as shown in drawing 5, a log in reception place transmits the frame called LS_RJT504 to log in demand origin to the PLOGI frame 503.

[0021] If the response of the ACC frame to the PLOGI frame which oneself transmitted is received, log in demand origin gets to know that the log in was successful, and will be in the condition that I/O processes, such as data transfer, can be started. Since a log in was not materialized when LS_RJT was received, the I/O process to a log in demand place becomes improper. Although the log in of a class 3 was described here, also in other log ins, it is same that *N_Port_Name*, *Node_Name*, and *S_ID* are contained in the information which can be passed to a log in demand place from log in demand origin.

[0022] Next, the Inquiry command is explained. The Inquiry command is a command which asks the mounting condition in advance of the case where it is going to start an I/O process, to the logical device set as the object of a process. For example, it is the thing of the information inquiry demand before the access request to the storage region included in storage subsystem from high order equipment. This command is a standard command surely supported in SCSI. [0023] Drawing 6 is a format of the frame 601 in the case of transmitting the Inquiry command defined by SCSI specification with the frame of fiber channel specification. In the detail structure 604 of the frame header 602, *S_ID*605 assigned by PLOGI before this frame is contained. There is a field called FCP_LUN607, FCP_CNTL608, FCP_CDB609, and FCP_DL610 in a data field 603. Here, FCP_LUN607 and FCP_CDB609 are described.

[0024] In FCP_LUN607, the identifier of the logical volume related with the port of a frame transmission place which frame transmitting origin tends to ask that a condition is stored. This identifier is called LUN. In FCP_CDB609, when using a SCSI commands set, the instruction information called a SCSI command description block (CDB) is stored. In this FCP_CDB609, the Inquiry command information on SCSI is stored and information is transmitted with above-mentioned FCP_LUN607 at a frame demand place.

[0025] Next, the information which answers frame transmitting origin as a response through which the frame demand place which received the Inquiry command asks and passes is described. This information is called Inquiry data. The extract of Inquiry data is shown in drawing 7. Here the KUOI fire 702 and two of the device type code 703 are described among the Inquiry data 701. A qualifier (Peripheral Qualifier) 702 is the information on the triplet which sets up the current condition of the specified Logical unit.

[0026] Drawing 8 enumerates the conditions of Logical unit shown with a bit pattern. It is shown that code 000 (binary) 802 are input/output equipment of a class with which the equipment connected as Logical unit is shown in the field of the device type code 703. Even if this code is

set up, it is not necessarily shown that the Logical unit is usable, i.e., a ready state, but when this code is set up, it restricts that the Logical unit may be able to be used.

[0027] It is shown that code 001 (binary) 803 are input/output equipment of a class with which the equipment connected as Logical unit is shown in the field of the device type code 703, and it is shown that a actual input/output equipment is not connected to the logical unit. This will show a case as [CD-ROM] it is not inserted into the drive, although the CD-ROM drive is mounted.

Code 011 (binary) 804 show that the specified Logical unit is not supported. Therefore, equipment is not assigned to the specified Logical unit. When this code is set up, it has been conditions that 1F (hexadecimal) are surely set to the device type coding region 703.

[0028] The device type code (Peripheral Device Type) 703 is 5-bit information which shows the classification of the input/output equipment actually assigned to the specified Logical unit.

[0029] The hexadecimal code 901 is shown for corresponding to drawing 9 at each device type 902. When 1F (hexadecimal) 904 which express the undefined or the non-connected device 903 among the information shown in drawing 9 are set up, the device which Inquiry command transmitting origin asked will be referred to as the undefined or un-connecting, and the Logical unit concerned can be used from the transmitting origin concerned.

[0030] The procedure of the Logical unit inquiry which used this Inquiry command for drawing 10 is shown. The high order equipment 1001 which is going to access Logical unit transmits the frame 1003 containing the Inquiry command to the storage subsystem 1002 with the Logical unit which it is going to access. LUN which is *S_ID* of the high order equipment assigned by PLOGI and the identifier of the Logical unit which performs an inquiry is contained in this frame. In addition, about LUN, it can set up also into the Inquiry command information in FCP_CDB itself besides a FCP_LUN field here. Although the effectiveness acquired whichever it uses a value is the same, in this example, the value of LUN shall use the value stored in FCP_LUN.

[0031] The storage subsystem 1002 which received the frame containing the Inquiry command transmits the frame 1004 which prepares Inquiry data required for the answerback to an inquiry, and contains the created Inquiry data to high order equipment. The frame which stores Inquiry data at this time is called FCP_DATA. When a qualifier 000 (binary) or device types 00~09 (hexadecimal) are set up about the logical unit (Logical unit) in which the inquiry had a storage subsystem at this time, the high order equipment which received this Inquiry data becomes possible [trying I/O to a logical unit].

[0032] Moreover, as shown in drawing 11, when the storage subsystem 1102 sets up a qualifier 001 (binary) or 011 (binary), and device type 1F (hexadecimal), the high order equipment which received this Inquiry data 1104 detects that I/O to a logical unit is impossible. It becomes possible from these things to control authorization and the disapproval of access to the logical unit from high order equipment by managing the qualifier stored in Inquiry data, and a device type code.

[0033] In this invention, it makes it possible to choose the fixed field in a storage subsystem as an object which permits or refuses access from high order equipment. This field is an addressable field clearly from high order equipment, and is called LU (Logical Unit). The identifier of LU is called LUN (Logical Unit Number). In SCSI-2, the number of LUN is per [8] one target.

[0034] Next, it explains that processing by this invention flows.

[0035] Drawing 12 is the block diagram of the equipment used as the example of this invention. This equipment is called the storage subsystem 1201. The storage subsystem 1201 is connected with high order equipment (it is called a host) 1203 by the port 1202 with two or more fiber channel interfaces. Although the topology is various, in order that it may not ask a topology by this invention by fiber channel agreement, it is put in block and written as a fiber channel 1204.

[0036] High order equipment 1203 is also equipped with one or more ports 1205 with a fiber

channel interface, and each port 1205 can communicate with the port 1202 and fiber channel

protocol on the storage subsystem 1201.

[0037] The storage subsystem 1201 has a central processing unit 1206, and performs various processings. Moreover, the storage subsystem 1201 equips the interior with nonvolatile memory 1207. This nonvolatile memory 1207 plays a role of a maintenance means to hold various tables, *N_Port_Name*, or *Node_Name*. The device drive control section 1208 is connected with the drive

device which has memorized information through a bus 1209. In this Fig., a drive device is regarded as a logical unit and it is displaying as Logical unit (LU) 1210. [0038] Moreover, the storage subsystem 1201 can have the communications control section 1211, and can perform transmission and reception of the communications control section 1214 of the equipment 1213 for maintenance, and information through a communication line 1212. It has [whose equipment 1213 for maintenance is] a central processing unit 1215, the input means 1216, and the display means 1217 like a personal computer. A user maintains the storage subsystem 1201 using this equipment 1213 for maintenance, and also sets up the information (access propriety table) which associated N_Port_Name or Node_Name, and the specific storage region of LU1210, and defined the access propriety to high order equipment 1203. Thus, the equipment 1213 for maintenance also plays the role of a setting means. Nonvolatile memory 1207 holds the access propriety table defined in this way with N_Port_Name or Node_Name. [0039] Furthermore, nonvolatile memory 1207 is an association table (when PLOGI which is the communication link demand to the storage subsystem 1201 from high order equipment 1203 is received) created with a central processing unit 1215. It is the information which can identify dynamically N_Port_Name or Node_Name, and high order equipment 1203 uniquely. The table which associated S_ID which is the value reported from high order equipment 1203 at the time of PLOGI, and was related with N_Port_Name or Node_Name which has held this S_ID in nonvolatile memory 1207 is held.

[0040] Drawing 13 explains the outline of the implementation approach of the LUIN security by this invention. First, in a procedure 1301, using N_Port_Name which a host has beforehand, a user creates the access propriety table which tied up N_Port_Name of LUN associated for every port of a storage subsystem, and the host who can access there using the equipment for maintenance (refer to drawing 12) etc., and holds to the storage regions in a storage subsystem (nonvolatile memory shown in drawing 12). N_Port_Name obtained here presupposes that it is known.

[0041] Next, in a procedure 1302, a host logs in to a storage subsystem. A storage subsystem takes out a host's N_Port_Name and S_ID from the PLOGI frame of this log in, and creates the association table which associated N_Port_Name and S_ID. The created association table is held like a previous access propriety table in the storage region in a storage subsystem.

[0042] Next, it moves to a procedure 1303, and a host transmits the Inquiry command, in order to inspect the condition of the Logical unit in a storage subsystem. The storage subsystem which received this Inquiry command takes out S_ID from the header of the frame which stores the Inquiry command, and is set from this frame as the object of the Inquiry command. And an association table is used, N_Port_Name is deduced from S_ID, and the information on whether the access permission of the LUN is further carried out from the access propriety table to N_Port_Name or it is disapproval is acquired.

[0043] A central processing unit judges access propriety in a procedure 1304 using the information on authorization or disapproval. When a result is authorization, in a procedure 1305, it sets it as Inquiry data that LU is mounting, and when it is disapproval, it sets up having not mounted LU in Inquiry data in a procedure 1307, and transmits to a host. The host who received Inquiry data analyzes data. Object LU is mounting, i.e., when it acquires from data that access to Object LU is permitted, as it is shown in a procedure 1306, the I/O demand to the LU concerned can be performed after it.

[0044] If it detects having not mounted Object LU, the I/O demand to the I/O demand to the LU concerned cannot be performed henceforth. The above procedure is able to realize management of the security to LU in a storage subsystem.

[0045] In addition, it is also the same as when Node_Name is used instead of N_Port_Name. Moreover, decision of access propriety forms not a central processing unit but the processor of dedication, and is good also as a decision means.

[0046] Next, each procedure is explained to a detail.

[0047] First, the table creation procedure of performing matching with N_Port_Name and LUN which are the first procedure is explained.

[0048] The security information over LUN in this invention shall be managed considering the port

which exists in a storage subsystem as a unit. That is, Logical unit LU is defined to each port, and a host accesses to LU through these ports. Therefore, security information will also be managed per port. In this case, required information is a status bit which shows the property of access to the information which can specify a host as a meaning, and LUN and LUN which are the identifier of each LU.

[0049] At this time, it becomes the information which can specify a host as a meaning with N_Port_Name. For every port which exists in a host, since N_Port_Name is a unique value, according to this invention, it can set up the security to LU in the port of a storage subsystem for every port of a host. If the table which used Node_Name is created instead of N_Port_Name, security will be set up for every host. Since it is a difference of whether the object which grants the access permission to LU is every port of a host, or you are every host, this example explains N_Port_Name. That is, although this example describes how to set up security for every port of a host, the security setting method of a host unit can be easily obtained by reading description of N_Port_Name as Node_Name. Moreover, in this example, the thing of the port on a host is made to call it a host for simplification. That is, the word of a host will mean the both sides of the port which exists on a host, or either as the host itself.

[0050] The access propriety table created by this example to drawing 14 is shown. This table is created for every port on a storage subsystem. From a storage subsystem and the equipment for maintenance which can be communicated, creation is performed by directing using the display means for checking an input means and its input result. If LAN is used and a setup from the location near a storage subsystem and the telephone line will be used according to the class of communication line, a maintenance center etc. can be set up from a remote place. Moreover, it is possible to also make the equipment for maintenance and a storage subsystem unify using an internal bus.

[0051] LU1402 shows LU related with the port, and only the number of the hosts who may access the number of N_Port_Name 1403 to LU which exists in the port subordinate exists. The number of LU and hosts turns into a limited number. In each element of a table, by this example, value '1' will mean an access permission and value '0' will mean access refusal. The host who has an access permission to LUN 0 in the port concerned in drawing 14 is N_Port_Name "0123456789ABCDEF" 1409. It is only the host who has and the host who has an access permission to LUN 1 1405 reaches N_Port_Name "8901234567 ABCDCE" 1410. He is a host with "01234567 89ABCDEF" 1411. Moreover, the host to whom access to LUN n-1 1407 is permitted does not exist.

[0052] As shown in drawing 15, this table is created about all ports to be set [of security] up, and is held to the storage region in a storage subsystem. If a non-volatilized storage region is used for a storage region at this time, information can be held even when the power source of a storage subsystem is disconnected. Moreover, table creation can be simplified by creating the table, using initial value as 0 or 1.

[0053] Next, the procedure of the log in from a host is explained to a detail. In this procedure, processing which connects a host's N_Port_Name and a host's S_ID is performed from the information accompanying PLOGI.

[0054] First, as shown in the procedure 1602 of drawing 16, the PLOGI frame is transmitted as a log in procedure from a host. In a procedure 1603, a host's S_ID is acquired from the header of the PLOGI frame with a storage subsystem. Moreover, to coincidence, a host's N_Port_Name is acquired from the data area of the PLOGI frame in a procedure 1604. In a procedure 1605, these two values are tied up and an association table as shown in drawing 17 is created. Since PLOGI is a log in exchanged between a host's port and the port on a storage subsystem, this table will also be created for every port of a storage subsystem.

[0055] By updating a table in a procedure 1606, it becomes possible to obtain N_Port_Name 1702 which corresponds if S_ID1701 is given using this table. It is the same as that of the table shown by drawing 14 that this table is also held in the storage region in a storage subsystem. To a host, the frame called ACC as a response to PLOGI in a procedure 1607 is transmitted, and it notifies that the log in was received by the host. The host who received the ACC frame can publish Inquiry to the port concerned etc. now henceforth.

[0056] Next, transmission of the Inquiry command from a host and the response of the security accompanying it are explained to a detail using drawing 18. The Inquiry command is transmitted to a storage subsystem from a host as a frame containing the information unit called FCP_CMND. The storage subsystem which received the FCP_CMND frame in the data field from a host in the procedure 1802 analyzes the contents of the FCP_CMND frame in a procedure 1803. When FCP_CMND is not the Inquiry command, it branches to the procedure 1805 according to each. When FCP_CMND is the Inquiry command, it changes for a procedure 1806 and S_ID is started from the frame concerned. Moreover, Inquiry takes out the target LUN from FCP_LUN in a procedure 1807 to coincidence.

[0057] Next, it moves to a procedure 1808 and N_Port_Name is calculated from S_ID started from the frame using the table shown by drawing 17. Furthermore, the Inquiry command acquires the condition of a bit which showed security about the target LUN from the table shown by drawing 14 about calculated N_Port_Name. S_ID obtained from the host at this time is FFFF01, and presupposes that LUN which Inquiry requires was 0. N_Port_Name "01234567 89ABCDEF" 1706 corresponding to S_IDFFF01 1703 from the table first shown in drawing 17 in a procedure 1808 It is N_Port_Name "01234567 89ABCDEF" 1409 from the table which moved to the procedure 1809 and was shown in drawing 14 after acquiring. Security of receiving LUN 0 1404 "1" It obtains.

[0058] Security "1" Since this example means an access permission, it branches for a procedure 1811 and the code corresponding to [corresponding to 000 (binary) to a qualifier] the device concerned to a device type is set as Inquiry data reported to a host. For example, a device type is set to 00 (hexadecimal) when a storage subsystem is a hard disk array subsystem.

Subsequently, the frame which stored Inquiry data is created and it transmits to a host in a procedure 1813. The frame called FCP_RSP which furthermore shows that the reply was completed in the procedure 1814 is transmitted to a host.

[0059] In order to mean that the host who received this reply data of a series of had detected that access was possible to the LU concerned of LUN=0 as a result of Inquiry, he becomes possible, accessing by not checking security to the LU concerned henceforth until it receives the next Inquiry command].

[0060] Next, the case where access is refused is explained. S_ID obtained from the host by transmission of the Inquiry command is FFFF01, and suppose that LUN which Inquiry requires was 1. Security of LUN 1 1405 [as opposed to N_Port_Name "01234567 89ABCDEF" 1409 from the access propriety table shown in drawing 14 after acquiring N_Port_Name "01234567 89ABCDEF" 1706 corresponding to S_IDFFF01 1703 from the association table shown in drawing 17 in a procedure 1808] "0" It obtains.

[0061] Security "0" Since this example means access refusal, it branches to a procedure 1812 and the Inquiry data which set 1F (hexadecimal) to the KU01 (binary) or 011 (binary), and a device type code are created as Inquiry data reported to a host. The host who received this Inquiry data and subsequently received FCP_RSP acquires the information that the LU concerned of LUN=1 has not been mounted as a result of Inquiry. Therefore, since a host judges henceforth that the LU concerned is not mounted, carrying out an access request is lost.

[0062] It can carry out efficiently by judging the security about access to each LUN to each port of a host for every port by the side of a storage subsystem by holding the table using N_Port_Name, S_ID, and LUN as mentioned above in the case of a log in and Inquiry.

[0063] [Effect of the Invention] The access propriety table of N_Port_Name or Node_Name which has set up access to Specification LUN beforehand from high order equipment by this invention, and LUN. By using the table of the both sides of the association table created using the relation between N_Port_Name or Node_Name which becomes clear in the case of PLOGI, and S_ID Since access propriety can be determined and it can answer when the condition inquiry to LU from the port of high order equipment or high order equipment is, the access restriction to a storage subsystem per LUN And it can carry out in a first-time judgment process, and security with the highest resolving power can be secured with high performance on a fiber channel and SCSI specification.

[Translation done.]

* NOTICES *

Japan Patent Office is not responsible for any damages caused by the use of this translation.

1. This document has been translated by computer. So the translation may not reflect the original precisely.
- 2.**** shows the word which can not be translated.
3. In the drawings, any words are not translated.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

- [Drawing 1] It is structural drawing of the frame in a fiber channel protocol.
- [Drawing 2] It is structural drawing of a frame header.
- [Drawing 3] It is structural drawing of the PLOGI frame.
- [Drawing 4] It is the sequence diagram where PLOGI is accepted.
- [Drawing 5] It is the sequence diagram where PLOGI is refused.
- [Drawing 6] It is structural drawing of the frame containing the SCSI Inquiry command.
- [Drawing 7] It is structural drawing of Inquiry data.
- [Drawing 8] It is the contents definition Fig. of the qualifier in Inquiry data.
- [Drawing 9] It is the contents definition Fig. of the device type code in Inquiry data.
- [Drawing 10] It is a sequence diagram in case LU normal state is set as Inquiry data.
- [Drawing 11] It is a sequence diagram in case LU undefined condition is set as Inquiry data.
- [Drawing 12] It is the block diagram of a storage subsystem.
- [Drawing 13] It is the flow chart of a whole sequence.
- [Drawing 14] It is the definition table of LU access propriety to N_Port_Name.
- [Drawing 15] It is the setting flow chart of LU access propriety definition table.
- [Drawing 16] It is the flow chart of PLOGI processing.
- [Drawing 17] It is the table which associates host N_Port_Name and S_ID.
- [Drawing 18] It is the flow chart of Inquiry command processing.

[Description of Notations]

101 — A frame, 102 — SOF (Start of Frame), 103 — A frame header, 104 — A data field, 105 — CRC, 106 — EOF (End of Frame), 201 — Frame, 202 — A frame header, 203 — A frame header detail, 204 — S_ID, 301 — A frame, 302 — A frame header, 303 — Data field, 304 — A frame header detail, 305 — A data field detail, 306 — S_ID, 307 — N_Port_Name, 308 — Node_Name, 401 — Actuation of log in demand origin, 402 — Actuation of a log in reception place, 403 — The contents of the PLOGI frame, 404 — The ACC frame, 501 — Actuation of log in demand origin, 502 — Actuation of a log in reception place, 503 — The contents of the PLOGI frame, 504 — LS_RJT frame, 601 — A frame, 602 — A frame header, 603 — Data field, 604 — A frame header detail, 605 — S_ID, 606 — Data field detail (FCP_CMND), 607 — FCP_LUN, 608 — FCP_CNTL, 609 — FCP_CDB (Inquiry), 610 — FCP_DL, 701 — An Inquiry data extract, 702 — Qualifier, 703 — A device type code, 801 — The definition of a qualifier, 802 — 000 (binary), 803—001 (binary), 804—011 (binary), 901 — A device type code (hexadecimal), 902 — Device type, 903 — 1F (hexadecimal), 904 undefined or a non-connected device, 1001 — The Inquiry processing sequence of high order equipment (host), 1002 — The Inquiry processing sequence of a storage subsystem, 1003 — Information stored in the frame (FCP_CMND) containing Inquiry, 1004 — The Inquiry data, 1101 which notify a device normal state — The Inquiry processing sequence of high order equipment (host), 1102 — The Inquiry processing sequence of a storage subsystem, 1103 — Information stored in the frame (FCP_CMND) containing Inquiry, 1104 — The Inquiry data, 1201 which notify a device undefined condition — Storage subsystem, 1202 — The fiber channel port of a storage subsystem, 1203 — High order equipment (host), 1204 — The fiber channel protocol which connects a storage subsystem with

a host, 1205 — A host's fiber channel port, 1206 — Central processing unit, 1207 — Nonvolatile memory, 1208 — A device drive control section, 1209 — Bus, 1210 — LU (Logical unit), 1211 — The communications control section, 1212 — Communication line, 1213 — The equipment for maintenance, 1214 — The communications control section, 1215 — Central processing unit, 1216 — An input means, 1217 — Display means, 1301 [— Whole procedures 4 and 1305 / — Whole procedures 5 and 1306 / — Whole procedures 6 and 1307 / — Whole procedures 7 and 1401 / — LU access propriety definition table, 1402 to N_Port_Name / — LUN,] — Whole procedures 1 and 1302 — Whole procedures 2 and 1303 — Whole procedures 3 and 1304 1403 — N_Port_Name, 1404 — The definition to LU of LUN 0, 1405 — The definition, 1406 to LU of LUN1 — The definition to LU of LUN 2, 1407 — The definition, 1408 to LU of LUN n-1 — The definition to LU of LUN n, 1409, 1410, 1411 — N_Port_Name, 1601 — PLOGI processing flow chart initiation, 1602 [— PLOGI procedure 4 and 1606 / — PLOGI procedure 5 and 1607 / — PLOGI procedure 6 and 1701 / — S_ID,] — PLOGI procedure 1 and 1603 — PLOGI procedure 2 and 1604 — PLOGI procedure 3 and 1605 1702 — N_Port_Name, 1703, 1704, 1705 — S_ID, 1706, 1707, 1708 — N_Port_Name, 1801 — Inquiry processing flow chart initiation, 1802 [— Inquiry procedure 4 and 1806 / — Inquiry procedure 5 and 1807 / — Inquiry procedure 6,] — Inquiry procedure 1 and 1803 — Inquiry procedure 2 and 1804 — Inquiry procedure 3 and 1805 1808 [— Inquiry procedure 10 and 1812 / — Inquiry procedure 11 and 1813 / — Inquiry procedure 12,] — Inquiry procedure 7 and 1809 — Inquiry procedure 8 and 1810 — Inquiry procedure 9 and 1811 1814 — Inquiry procedure 13.

[Translation done.]